WHITEPAPER

How the Gigamon Insight Solution Can Help Secure Medical Devices

In October 2018, the Food and Drug Administration (FDA), in collaboration with MITRE Corporation, released the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. The document was published to assist Healthcare Delivery Organizations (HDOs) with preparedness and response when it comes to cybersecurity threats affecting medical devices.

Securing medical devices continues to be a challenge for HDOs because many of the devices are running outdated operating systems, have unpatched vulnerabilities, and contain insecure protocols. Regulations can require a lengthy device certification process to ensure proper device functionality specific to the installed operating system and patch level; the HDO can be liable for non-adherence. Changes in either the operating system or patch level may require re-certification; the associated time and expense needed to complete this is not optimal. In addition, many of these devices are not designed to support addtional security software installed on them such as endpoint security software often installed on most consumer devices. As a consequence, more and more, HDOs are turning to nonintrusive network-based security solutions to passively monitor and detect threats on their medical devices.

The playbook published by the FDA and MITRE follows the National Institute of Standards and Technology's (NIST) incident response lifecycle outlined in their publication of *Computer Security Incident Handling Guide* (800-61r2). The lifecycle contains four phases: Preparation, Detection & Analysis, Containment Eradication & Recovery, and Post-incident Activity.

The Gigamon Insight™ solution supports an organization's ability to protect their network by providing the means to effectively detect, investigate and respond to cybersecurity threats that are currently challenging HDOs.

Preparation Phase

Section 6.1.2 – Medical Device Asset Inventory

WHAT THE PLAYBOOK SAYS:
The playbook refers to gathering and maintaining information about the medical devices on the HDO's network.

HOW INSIGHT SOLUTION HELPS:
Insight sensors deployed within the HDO's network collect the network traffic to/from the medical devices and extract rich metadata, which is then stored in a centralized SaaS repository. This metadata contains some of the information necessary to inventory these medical devices. Information such as the Internet Protocol (IP) address and network protocols can be used to identify and inventory medical devices.

Section 6.1.3 – Hazard Vulnerability Analysis

WHAT THE PLAYBOOK SAYS:
This section recommends performing a Hazard Vulnerability Analysis (HVA) to gauge the potential impact of a cybersecurity incident affecting medical devices, and then perform mitigation of identified risks. One such potential risk that may be identified is "Limited sensor coverage to detect adversary activity of HDO devices, other systems, and networks".

HOW INSIGHT SOLUTION HELPS:
The Insight solution's network sensors are designed to be deployed rapidly and to scale up or down as needs shift. Sensors are fully managed and can be deployed in minutes across a variety of environments. This enables HDOs to arm their incident responders with the network visibility of medical devices necessary to effectively detect, respond, and investigate cybersecurity incidents.

© 2019 Gigamon. All rights reserved.

Detection & Analysis Phase

Section 6.2.1 – Incident Detection and Validation

WHAT THE PLAYBOOK SAYS:
Detection of cybersecurity incidents can be a challenge for any organization, especially as attackers' tactics to remain unnoticed become more and more sophisticated. Even with a fully staffed team of cybersecurity specialists, many HDO's find it difficult to keep up with the ever-changing cybersecurity threat landscape. Assistance is needed to create, qualify, and maintain methods for threat detection.

HOW INSIGHT SOLUTION HELPS:
Insight provides HDOs with an automated detection engine that can immediately notify security teams when a cybersecurity incident is observed through the inspection of network event metadata. To assist HDO's with detections, Gigamon Applied Threat Research (ATR) is continuously crafting and qualifying a set of high-fidelity managed detections designed to identify attacker behaviors and patterns. The Insight solution also offers HDOs the ability to create their own customized detections specific to their environment to monitor and detect unexpected or unwanted adversarial activity.

Section 6.2.2 – Incident Categorization and Prioritization

WHAT THE PLAYBOOK SAYS:
The Incident Categorization and Prioritization step is a critical one in the incident response lifecycle, however determining the severity of a cybersecurity incident and setting the appropriate priority can be challenging.

HOW INSIGHT SOLUTION HELPS:
Insight is designed to assist incident responders in dealing with this by providing both a guidance on category, severity, and priority for each detection. When Gigamon ATR crafts a new detection ruleset, they provide a threat category, severity level, and confidence level. Categories are mapped to the MITRE ATT&CK framework whenever possible, so incident responders can easily determine the type of incident that was detected. Severity levels are based on the potential business impact of the threat, while confidence levels are based on the accuracy of the detection pattern. The severity and confidence levels provide incident responders with an accurate way to determine priority of detected cyber security incidents on all devices on the network.

Section 6.2.4 – Incident Analysis

WHAT THE PLAYBOOK SAYS:
During the incident investigation it is important to determine the full incident impact, which includes the scope of the impacted devices. The playbook recommends using both internal and external sources to provide additional context for incident responders to effectively investigate and analyze the incident.

HOW INSIGHT SOLUTION HELPS:
Insight detections are designed to provide incident responders with a view of all currently impacted devices for a given detection. This consolidated view allows the incident responder to investigate multiple impacted devices at the same time and provide time context around the network events. The Insight solution's entity enrichment provides incident responders with information collected from both external and internal sources during the investigation. External enrichment includes information about external IP addresses (WHOIS) and matches on threat intelligence sources. Internal enrichment is extracted from the collected network traffic and includes user login data, software and application information, and more.

6.4.2 – Forensic Investigation

WHAT THE PLAYBOOK SAYS:
Post-analysis forensic investigation may be necessary to determine the full extent of damages caused by the security incident.

HOW INSIGHT SOLUTION HELPS:
The Insight solution provides incident responders with the ability to perform targeted packet capture of the network traffic on the impacted devices.

© 2019 Gigamon. All rights reserved.

Conclusion

As the number of medical devices being used in HDOs' networks increase, so too does the number of targets for threat actors. Security teams need a way to quickly and easily guard these medical devices from the onslaught of cybersecurity threats. A passive network security monitoring solution like the Gigamon Insight solution is an effective way for HDO's to not only cover the existing medical devices in their network, but also any new devices that are placed onto the network. Insight can help HDOs adhere to the recommendations put forth by the FDA in this latest security preparedness playbook, by providing the visibility coverage they require to secure these medical devices. This provides security teams with the means to effectively detect and respond to cybersecurity threats that are currently challenging HDOs.

About Gigamon

Gigamon® is the recognized leader in network visibility solutions, delivering the powerful insights needed to see, secure and empower enterprise networks. Our solutions accelerate threat detection and incident response while empowering customers to maximize their infrastructure performance across physical, virtual and cloud networks. Since 2004 we have cultivated a global customer base which includes leading service providers, government agencies as well as enterprise NetOps and SecOps teams from more than 80 percent of the Fortune 100.

The MITRE Corporation. (2018). Medical Device Cybersecurity [PDF file]. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf

© 2019 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com